View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by CERN Document Server

arXiv:quant-ph/0702129v1 13 Feb 2007

Quantum expanders and the quantum entropy difference problem

Avraham Ben-Aroya * *Amnon Ta-Shma* *

Abstract

Classical expanders and extractors have numerous applications in computer science. However, it seems these classical objects have no meaningful quantum generalization. This is because it is easy to generate entropy in quantum computation simply by tracing out registers.

In this paper we define quantum expanders and extractors in a natural way. We show that this definition is exactly what is needed for showing that QED, the quantum analogue of ED (the entropy difference problem) is QSZK-complete.

We also show that quantum expanders exist and with very good parameters in the high min-entropy regime. The first construction is derived from the work of Ambainis and Smith and is based on expander graphs that are based on Cayley graphs of Abelian groups. The drawback of this construction is that it uses logarithmic seed length (yet, this already suffices for showing that QED is QSZK-complete).

We also show a quantum analogue of the Lubotzky, Philips and Sarnak construction of Ramanujan expanders from Cayley graphs of PGL$(2, q)$. Our construction is a sequence of two steps on the Cayley graph with a basis change in between steps. We believe this quantum analogue of classical Ramanujan expanders is of independent interest.

1 Introduction

1.1 Conductors

Expanders are sparse graphs in which every not too large set expands. Condensers are hash functions from a large domain to a much smaller one, that preserve the entropy of every (not too large) input distribution. Deterministic condensers do not exist, but using little fresh randomness, very good condensers exist. Extractors and dispersers are hash functions that transform any distribution with enough entropy to close to the uniform distribution. Again, extractors and dispersers have to use (little) fresh randomness. These and other objects fall under the general definition of "conductors" [CRVW02]. These objects have numerous applications in computer science, in many different areas including error correcting codes, derandomization, lower bound proofs, databases, communication networks, zero knowledge and more.

It is natural to look for quantum analogues of these notions. For example, an extractor is a deterministic transformation $E : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$, with the property that if the input x is drawn from a probability distribution over $\{0,1\}^n$ with min-entropy k, and if y is drawn from an independent and uniform distribution, then the output distribution is close to uniform. The output distribution should contain as much entropy as possible (ideally close to $k + d$).

A natural attempt to generalize this notion is to say a quantum extractor is a superoperator $T : L(V) \times L(R) \to L(M)$ with the property that for every $\rho \in D(V)$ with $H_\infty(\rho) \geq k$, the output density matrix $T(\rho \otimes \tilde{I}_R)$ is close to $\tilde{I}_M$, where $\tilde{I}_X = \frac{1}{dim(X)} I$ is the completely mixed state over the Hilbert space X. However, this notion is problematic because a superoperator can create entropy out of nowhere, by using ancilla and applying measurements. In particular, T can ignore its input, and create $\tilde{I}_M$ itself.

In this paper we suggest what we believe is a natural definition for quantum conductors. We then discuss whether these quantum objects exist at all, show some constructions and use it to prove that QED is QSZK-complete.

*School of Computer Science, Tel Aviv University, Tel Aviv 69978,Israel. E–mail: {abrhambe,amnon}@tau.ac.il

1.2 Quantum expanders

Classical expanders can be defined combinatorially or algebraically. In the combinatorial definition the requirement is that every not too large set expands. The algebraic definition, however, views the graph as an operator defined by the adjacency matrix of the graph. A graph is a good expander if the operator has a large spectral gap. Such an expander, in particular, implies combinatorial expansion (this claim is usually known as the mixing lemma). However, the algebraic definition guarantees even entropic expansion, i.e., every distribution with not too large min-entropy is mapped to a new distribution with higher min-entropy. The combinatorial definition then corresponds to dealing with distributions whose support is flat on a set of elements (i.e., all elements in the set get equal weight).

We extend the algebraic definition to the quantum setting. Intuitively, we would like to define a quantum expander as a superoperator T that has the completely mixed state $\tilde{I}$ as an eigenvector with eigenvalue 1, and has a large spectral gap. However, we also want to rule-out, e.g., the superoperator that on any input ρ outputs the completely mixed state $\tilde{I}$. In the classical setting this is done by requiring that the expander graph has a small degree D. In our setting, we translate this to the requirement that no matter what the input ρ is, $T(\rho)$ does not have more then d entropy more than ρ, i.e., the superoperator T does not introduce much min-entropy to the process on its own.

Definition 1. *An admissible superoperator $T : L(V) \to L(V)$ is a $(D = 2^d, \overline{\lambda})$ expander if:*

- *$T(\tilde{I}) = \tilde{I}$ and the eigenspace of eigenvalue 1 has dimension 1.*
- *For any $A \in L(V)$ that is orthogonal to $\tilde{I}$ (with respect to the Hilbert-Schmidt inner product, i.e. $\mathrm{Tr}(A\tilde{I}) = 0$) it holds that $\| T(A) \| \leq \overline{\lambda} \| A \|$.*
- *For every $\rho \in D(V)$ we have $S(T(\rho)) \leq S(\rho) + d$.*

A quantum expander is explicit if T can be implemented by a polynomial size circuit.

An alternative (and equivalent) definition would replace the second condition by a condition on the singular values of T.

In this terminology one can interpret the work of Ambainis and Smith [AS04] as giving the following:

Lemma 1.1. *[AS04] There exists an explicit $(\frac{O(\log N)}{\overline{\lambda}^2}, \overline{\lambda})$ quantum expander $T : L(V) \to L(V)$ and where $dim(V) = N$.*

Their quantum expander is based on a classical expander that is based on the Abelian group $\mathbb{Z}_2^n$. The main problem with Abelian expanders is that it is impossible to get a constant degree Cayley expander. This is reflected in the $O(\log N)$ term above. Lemma 1.1 suffices for showing that QED is QSZK-complete, but here we try to get the quantum analogue of the constant degree Ramanujan expanders of [LPS88]. This expander is a Cayley graph over the non-Abelian group $\mathrm{PGL}(2, q)$. Indeed, we give a construction that is based on the [LPS88] construction and prove:

Theorem 1.1. *There exists a $(D = O(\frac{1}{\overline{\lambda}^4}), \overline{\lambda})$ quantum expander.*

Our construction is not explicit in the sense that it uses the Fourier transform over PGL(2,q), which is not known to have an efficient implementation.

The PGL(2,q) quantum expander is as follows: we take two steps on the expander graph, with a basis change between each of the steps. The basis change is a carefully chosen transformation. It is a refinement of the Fourier transformation that maps the standard basis $|g\rangle$ of the group algebra $\mathbb{C}[\mathrm{PGL}(2, q)]$ to the basis of the irreducible, invariant subspaces of $\mathrm{PGL}(2, q)$. However, choosing the right refinement is not an easy task. Intuitively, the basis change is needed for dealing with both the bit and the phase levels, and is similar to the construction of quantum error correcting codes by first applying a classical code in the standard basis and then in the Fourier basis. However, things get complicated because we deal with non-Abelian groups. For doing the analysis (and concluding that two steps suffice) we need to use the structure of the group PGL(2,q). In particular, we use the specific structure of its subgroups and its irreducible representations (we use only the number of irreducible representations of each dimension).

1.3 Quantum extractors

We similarly define quantum extractors as follows:

Definition 2. *Let V, W be Hilbert spaces of dimensions N, M respectively. A superoperator $T : L(V) \to L(W)$ is a (k, d, ϵ)* quantum extractor, *if the following two conditions hold:*

- *For every $\rho \in D(V)$ with $H_2(\rho) \geq k$ we have $\left\| T\rho - \tilde{I} \right\|_{\mathrm{tr}} \leq \epsilon$, where $\tilde{I} = \frac{1}{N} I$, and,*
- *For every $\rho \in D(V)$ we have $S(T\rho) \leq S(\rho) + d$.*

If $W = V$ we see the extractor is balanced. *We say T is efficient If T can be implemented by a polynomial-size quantum circuit.*

Note that the use of Renyi entropy instead of min-entropy in the first condition only strengthens the definition, because for any $\rho \in D(V)$, $H_2(\rho) \geq H_\infty(\rho)$.

We suspect that *unbalanced* quantum extractors (where $N > \sqrt{M}$) do not exist. Never the less, we prove that very good *balanced*, quantum extractors exist. We prove:

Lemma 1.2. *If $T : L(V) \to L(V)$ is a $(D = 2^d, \overline{\lambda})$ quantum expander, then for every $t > 0$, T is also a $(k = n - t, d, \epsilon)$ quantum extractor with $\epsilon = 2^{t/2} \cdot \overline{\lambda}$.*

The Lemma is a generalization of a well known classical claim (e.g., [GW97]). We prove it in Section 2.4. In particular, we get an $(n-t, d, \epsilon)$ balanced quantum extractor $T : L(V) \to L(V)$ where $n = dim(V)$, and

- $d = t + 2\log(\frac{1}{\epsilon}) + 2\log(n) + O(1)$ using the Ambainis Smith quantum expander. In this case the quantum extractor is also *explicit*.
- $d = 2(t + 2\log(\frac{1}{\epsilon})) + O(1)$ using the PGL(2,q) quantum expander. Here the construction is *non-explicit*, because we do not know how to efficiently implement the Fourier transform of PGL(2,q).

1.4 QSZK

Watrous [Wat02] defined the notion of quantum statistical zero knowledge proofs. He considered the Quantum State Distinguishability promise problem ($QSD_{\alpha,\beta}$), which given two quantum circuits Q_0, Q_1, accepts if $\| \, |Q_0\rangle - |Q_1\rangle \, \|_{\mathrm{tr}} \geq \beta$ and rejects if $\| \, |Q_0\rangle - |Q_1\rangle \, \|_{\mathrm{tr}} \leq \alpha$. The notation $|Q\rangle$ denotes the mixed state obtained by running Q on the state $|0^n\rangle$ and tracing out the non-output qubits. Watrous showed $\mathrm{QSD}_{\alpha,\beta}$ is complete for honest-verifier-QSZK ($\mathrm{QSZK_{HV}}$) when $0 \leq \alpha < \beta^2 \leq 1$. He further showed that $\mathrm{QSZK_{HV}}$ is closed under complement, that any problem in $\mathrm{QSZK_{HV}}$ has a 2 message proof system and a 3 message public-coin proof system and also that QSZK $\subseteq$ PSPACE. Subsequently, in [Wat06], he showed that $\mathrm{QSZK_{HV}} = \mathrm{QSZK}$.

The above results have classical analogues. However, in the classical setting there is another canonical complete problem, the Entropy Difference problem (ED). There is a natural quantum analogue to ED, the Quantum Entropy Difference problem (QED), that given two quantum circuits Q_0, Q_1 as inputs, accepts if $S(|Q_0\rangle) - S(|Q_1\rangle) \geq \frac{1}{2}$ and rejects if $S(|Q_1\rangle) - S(|Q_0\rangle) \geq \frac{1}{2}$ (where $S(\rho)$ is the Von-Neumann entropy of the mixed state ρ). We show in this paper that QED is QSZK-complete.

The classical proof that ED is SZK-complete uses *extractors*. As we will see in the paper, our definition turns out to be exactly what is needed for showing that QED is QSZK-complete.

1.5 Summary and organization

To conclude, our contributions are:

- We define quantum expanders and extractors in a natural way.
- We show constant-seed quantum expanders exist, giving a quantum analogue of the [LPS88] constant-degree classical expander.
- We show that QED is QSZK-complete.
- We show that QSZK is closed under boolean formula.

After the preliminaries (Section 2), we explain in Section 3 how to build the PGL(2,q) quantum expander. The second part of the paper is devoted to proving the completeness of QED in QSZK. Much of the work done here (but not all) is an adaptation of the results and techniques of the classical world to the quantum setting. The proof that QED is in QSZK appears in Section 4. The proof uses a lemma relating entropy to distance from uniform, which appears in Section 5. Also, the proof uses another problem, quantum entropy approximation, and its relation to QED is discussed in Section 7. For this part we need the closure of QSZK under Boolean formula that is discussed in Section 6. The reduction from QSD to QED appears in Section 8. We discuss some open problems in Section 9.

2 Preliminaries

2.1 Entropy of a density matrix

We first define the classical Renyi entropy. Let $P = (p_1, \ldots, p_m)$ be a classical probability distribution.

- The *Shannon entropy* of P is $H(P) = \sum_{i=1}^{m} p_i \lg \frac{1}{p_i}$.
- The *min-entropy* of P is $H_\infty(P) = \min_i \lg \frac{1}{p_i}$.
- The *Renyi entropy* of P is $H_2(P) = \lg \frac{1}{\mathrm{Col}(P)}$, where $\mathrm{Col}(P) = \sum p_i^2$ is the collision probability of the distribution defined by $\mathrm{Col}(P) = \Pr_{x,y}[x = y]$ when x, y are sampled from P.

Now let $\rho \in D(V)$ be a density matrix (where V is a Hilbert space, $L(V)$ is the set of linear operators over V and $D(V)$ is the set of positive semi-definite operators in $L(V)$ with trace 1, i.e., all density matrices over V). Let $\alpha = (\alpha_1, \ldots, \alpha_N)$ be the set of eigenvalues of ρ. Since ρ is positive semi-definite, all these eigenvalues are non-negative. Since $\mathrm{Tr}(\rho) = 1$ their sum is 1. Thus we can view α as a classical probability distribution. We define:

- The *von Neumann entropy* of ρ is $S(\rho) = H(\alpha)$.
- The *min-entropy* of ρ is $H_\infty(\rho) = H_\infty(\alpha)$.
- The *Renyi entropy* of ρ is $H_2(\rho) = H_2(\alpha)$.

The analogue of the collision probability is simply $\mathrm{Tr}\,\rho^2 = \sum_i \alpha_i^2 = ||\rho||^2$.

Fact 2.1. *For any distribution P, $H_\infty(P) \le H_2(P) \le H(P)$ and $2H_\infty(P) \ge H_2(P)$.*

Lemma 2.1. *Let T be a normal linear operator with eigenspaces $V_1, \ldots, V_n$ and corresponding eigenvalues $\lambda_1, \ldots, \lambda_n$ in descending* absolute *value. Suppose u and w are vectors such that $u \in \mathrm{Span}\,\{V_2, \ldots, V_n\}$ and $w \perp u$ (w does not necessarily belong to V_1). Then*

$$||(T(u + w))||^2 \le |\lambda_2|^2 ||u||^2 + |\lambda_1|^2 ||w||^2.$$

Proof. Let $\{v_j\}$ be an eigenvector basis for T with eigenvalues δ_j (from the set $\{\lambda_1, \ldots, \lambda_n\}$). Writing $u = \sum_j \alpha_j v_j$ and $w = \beta v + \sum_j \beta_j v_j$ with $v_j \in \mathrm{Span}\{V_2, \ldots, V_n\}$ and $v \in V_1$, we get:

$$
\begin{aligned}
||T(u+v)||^2 &= ||\lambda_1 \beta v + \sum_j \delta_j (\alpha_j + \beta_j) v_j||^2 \\
&= |\lambda_1|^2 |\beta|^2 + \sum_j |\delta_j|^2 |\alpha_j + \beta_j|^2 \\
&\leq |\lambda_1|^2 |\beta|^2 + |\lambda_2|^2 \sum_j |\alpha_j + \beta_j|^2 \\
&= |\lambda_1|^2 |\beta|^2 + |\lambda_2|^2 (\sum_j |\alpha_j|^2 + \sum_j |\beta_j|^2 + \sum_j (\alpha_j^* \beta_j + \alpha_j \beta_j^*)) \\
&= |\lambda_1|^2 |\beta|^2 + |\lambda_2|^2 (\sum_j |\alpha_j|^2 + \sum_j |\beta_j|^2) \\
&\leq |\lambda_1|^2 (|\beta|^2 + \sum_j |\beta_j|^2) + |\lambda_2|^2 \sum_j |\alpha_j|^2 = |\lambda_2|^2 ||u||^2 + |\lambda_1|^2 ||w||^2.
\end{aligned}
$$

where in the calculation we used the fact that $\sum_j \alpha_j^* \beta_j = \langle u|v \rangle = 0$ because of the orthogonality of u and w. □

The proof of the following facts can be found in [NC00].

Fact 2.2. ***(Joint entropy theorem)*** *Suppose p_i are probabilities, $|i\rangle$ are orthogonal states for a system A, and ρ_i is any set of density operators for another system B. Then*

$$S\left(\sum_i p_i |i\rangle\langle i| \otimes \rho_i\right) = H(p_i) + \sum_i p_i S(\rho_i).$$

Fact 2.3. ***(Fannes' inequality)*** *Suppose ρ and σ are density matrices over a Hilbert space of dimension d. Suppose further that the trace distance between them satisfies $t = \| \rho - \sigma \|_{\mathrm{tr}} \leq 1/e$. Then*

$$|S(\rho) - S(\sigma)| \leq t(\ln d - \ln t).$$

The following lemma is taken from [ANTSV02]. It can be proved using Holevo's bound.

Lemma 2.2. ***(Lemma 3.2, [ANTSV02])*** *Let ρ_0 and ρ_1 be two density matrices, and let $\rho = \frac{1}{2}(\rho_0 + \rho_1)$. If there exists is a measurement with outcome 0 or 1 such that making the measurement on ρ_b yields the bit b with probability at least p, then*

$$S(\rho) \geq \frac{1}{2}[S(\rho_0) + S(\rho_1)] + (1 - H(p)).$$

2.2 Trace distance

The *statistical difference* between two classical distributions $P = (p_1, \ldots, p_m)$ and $Q = (q_1, \ldots, q_m)$ is $\mathrm{SD}(P, Q) = \frac{1}{2} \sum_{i=1}^m |p_i - q_i|$, i.e., half the ℓ_1 norm of $P - Q$. This can be generalized to the quantum world by defining the trace-norm of a matrix $X \in L(V)$ to be $\| X \|_{\mathrm{tr}} = Tr(|X|)$, where $|X| = \sqrt{XX^\dagger}$, and defining the *trace distance* between density matrices ρ and σ to be $\frac{1}{2} \| \rho - \sigma \|_{\mathrm{tr}}$.

In the classical world $SD(P, Q) = \max_S P(S) - Q(S)$, i.e., it describes the maximal probability with which one can distinguish the two distributions. The trace distance achieves the same for density matrices, as is captured in:

Fact 2.4. *(e.g., [NC00]) Let ρ_0 and ρ_1 be two density matrices. Then there exists a measurement $\mathcal{O}$ with outcome 0 or 1 such that making the measurement on ρ_b yields the bit b with probability $\frac{1}{2} + \frac{\| \rho_0 - \rho_1 \|_{\rm tr}}{2}$. Furthermore, no measurement can distinguish the two density matrices better.*

Combining the last fact with Lemma 2.2 we get

Lemma 2.3. *Let ρ_0 and ρ_1 be two density matrices, and let $\rho = \frac{1}{2}(\rho_0 + \rho_1)$. Then*

$$S(\rho) \geq \frac{1}{2}[S(\rho_0) + S(\rho_1)] + (1 - H(\frac{1}{2} + \frac{\| \rho_0 - \rho_1 \|_{\rm tr}}{2})).$$

As with classical distributions, the distance between density matrices can only decrease with computation, i.e.,

Fact 2.5. *([NC00]) Let ρ_0 and ρ_1 be two density matrices. Then for any quantum operation $\mathcal{E}$ it holds that $\| \mathcal{E}(\rho_0) - \mathcal{E}(\rho_1) \|_{\rm tr} \leq \| \rho_0 - \rho_1 \|_{\rm tr}$.*

Finally, we need the following simple facts:

1. For any Hermitian matrix T, $\| T \|_{\rm tr} \leq \sqrt{N} \cdot ||T||^2$ (by a simple Cauchy-Schwartz).
2. $\| X \otimes Y \|_{\rm tr} = \| X \|_{\rm tr} \cdot \| Y \|_{\rm tr}$ ([NC00])

2.3 The polarization lemma

We will require a theorem of Watrous [Wat02] (based on the work of [SV97] on SD) regarding a way to manipulate trace distance.

Theorem 2.1. ***(Polarization lemma, Theorem 5 at [Wat02])*** *Let α and β satisfy $0 \leq \alpha < \beta^2 \leq 1$. Then there is a deterministic polynomial-time procedure that, on input $(Q_0, Q_1, 1^n)$ where Q_0 and Q_1 are quantum circuits, outputs descriptions of quantum circuits (R_0, R_1) (each having size polynomial in n and in the size of Q_0 and Q_1) such that*

$$\begin{aligned} \| |Q_0\rangle - |Q_1\rangle \|_{\rm tr} \leq \alpha \quad &\Rightarrow \quad \| |R_0\rangle - |R_1\rangle \|_{\rm tr} \leq 2^{-n}, \\ \| |Q_0\rangle - |Q_1\rangle \|_{\rm tr} \geq \beta \quad &\Rightarrow \quad \| |R_0\rangle - |R_1\rangle \|_{\rm tr} \geq 1 - 2^{-n}. \end{aligned}$$

2.4 Quantum expanders and extractors

Proof. (Of Lemma 1.2) T has an dimension 1 eigenspace with eigenvalue 1, with the norm 1 eigenvector $v_1 = \frac{1}{\sqrt{N}} I$ (where $dim(V) = N$). Our input ρ is a density matrix and therefore $\langle \rho \mid v_1 \rangle = \frac{1}{\sqrt{N}} \operatorname{Tr}(\rho) = \frac{1}{\sqrt{N}}$. In particular $\rho - \frac{1}{\sqrt{N}} v_1 = \rho - \tilde{I}$ is perpendicular to the eigenvalue 1 eigenspace. Therefore,

$$\begin{aligned} ||T(\rho) - \tilde{I}||^2 &= ||T(\rho - \tilde{I})||^2 \leq \overline{\lambda}^2 ||\rho - \tilde{I}||^2 \\ &= \overline{\lambda}^2 [||\rho||^2 - \langle \rho | \tilde{I} \rangle - \langle \tilde{I} | \rho \rangle + ||\tilde{I}||^2] = \overline{\lambda}^2 [||\rho||^2 - \frac{1}{N}] \leq \overline{\lambda}^2 ||\rho||^2. \end{aligned}$$

Plugging $H_2(\rho) \geq k = n - t$ we see that $||T(\rho) - \tilde{I}||^2 \leq \overline{\lambda}^2 2^{-(n-t)}$. Using Cauchy-Schwartz

$$\begin{aligned} \left\| T(\rho) - \tilde{I} \right\|_{\rm tr} &\leq \sqrt{N} ||T(\rho) - \tilde{I}|| \\ &\leq \sqrt{N} \cdot \overline{\lambda} \cdot 2^{-\frac{n-t}{2}} = 2^{t/2} \cdot \overline{\lambda} = \epsilon. \end{aligned}$$

□

2.5 Representation Theory Background

We survey some basic elements of representation theory. For complete accounts, consult the books of Serre [Ser77] or Fulton and Harris [HF91]. The exposition below heavily uses the one given in [HRTS00].

A representation ρ of a finite group G is a homomorphism $\rho : G \to \mathrm{GL}(V)$, where V is a (finite-dimensional) vector space over $\mathbb{C}$ and $\mathrm{GL}(V)$ denotes the group of invertible linear operators on V. Fixing a basis for V, each $\rho(g)$ may be realized as a $d \times d$ matrix over $\mathbb{C}$, where d is the dimension of V. As ρ is a homomorphism, for any $g, h \in G$, $\rho(gh) = \rho(g)\rho(h)$ (this second product being matrix multiplication). The *dimension* d_ρ of the representation ρ is d, the dimension of V.

We say that two representations $\rho_1 : G \to \mathrm{GL}(V)$ and $\rho_2 : G \to \mathrm{GL}(W)$ of a group G are *isomorphic* when there is a linear isomorphism of the two vector spaces $\phi : V \to W$ so that for all $g \in G$, $\phi\rho_1(g) = \rho_2(g)\phi$. In this case, we write $\rho_1 \cong \rho_2$. Up to isomorphism, a finite group has a finite number of irreducible representations; we let $\hat{G}$ denote this collection (of representations).

We say that a subspace $W \subset V$ is an *invariant* subspace of a representation $\rho : G \to \mathrm{GL}(V)$ if $\rho(g)W \subseteq W$ for all $g \in G$. The zero subspace and the subspace V are always invariant. If no nonzero proper subspaces are invariant, the representation is said to be *irreducible*.

If $\rho : G \to \mathrm{GL}(V)$ is a representation, $V = V_1 \oplus V_2$ and each V_i is an invariant sub-space of ρ, then $\rho(g)$ defines two linear representations $\rho_i : G \to \mathrm{GL}(V_i)$ such that $\rho(g) = \rho_1(g) + \rho_2(g)$. We then write $\rho = \rho_1 \oplus \rho_2$. Any representation ρ can be written $\rho = \rho_1 \oplus \rho_2 \oplus \ldots \oplus \rho_k$, where each ρ_i is irreducible. In particular, there is a basis in which every matrix $\rho(g)$ is block diagonal, the ith block corresponding to the ith representation in the decomposition. While this decomposition is not, in general, unique, the *number* of times a given irreducible representation appears in this decomposition (up to isomorphism) depends only on the original representation ρ.

A representation ρ of a group G is also automatically a representation of any subgroup H. We refer to this *restricted* representation on H as $\mathrm{Res}_H \rho$. Note that even representations that are irreducible over G may be reducible when restricted to H.

Let G be an Abelian group of cardinality N. The group algebra $\mathbb{C}[G]$ of G is a vector space of dimension N over $\mathbb{C}$, with an orthonormal basis $\{|g\rangle \mid g \in G\}$ and multiplication $\sum a_g |g\rangle \cdot \sum b_{g'} |g'\rangle = \sum_{g,g'} a_g b_{g'} |g \cdot g'\rangle$. The group algebra is isomorphic to the set $\{f : G \to \mathbb{C}\}$ with the isomorphism being $f \to \sum_g f(g) |g\rangle$. The inner product in $\mathbb{C}[G]$ translates to the familiar inner product $\langle f, h\rangle = \sum_g \overline{f(g)} h(g)$. The regular representation $\rho_{\mathrm{reg}} : G \to \mathrm{GL}(V)$ is defined by $\rho_{\mathrm{reg}}(s) : e_x \mapsto e_{sx}$, for any $x \in G$. V has dimension $|G|$ and, with the basis above, $\rho_{\mathrm{reg}}(g)$ is a permutation matrix for any $g \in G$.

An interesting fact about the regular representation is that it contains every irreducible representation of G. In particular, if $\rho_1, \ldots, \rho_k$ are the irreducible representations of G with dimensions $d_{\rho_1}, \ldots, d_{\rho_k}$, then

$$\rho_{\mathrm{reg}} = d_{\rho_1}\rho_1 \oplus \cdots \oplus d_{\rho_k}\rho_k,$$

so that the regular representation contains each irreducible representation ρ exactly d_ρ times.

In the quantum setting we identify e_g with $|g\rangle$, and the function $f : G \to \mathbb{C}$ with the state $\sum_{g\in G} f(g) |g\rangle$. In this notation the linear transformation $\rho_{\mathrm{reg}}(s)$ is $\rho_{\mathrm{reg}}(g) = \sum_x |sx\rangle\langle x|$.

The *Fourier transform* over G is a unitary transformation F mapping the standard basis $\{|g\rangle : g \in G\}$ to the basis of the invariant subspaces of ρ_{reg}. That is for any $g \in G$ the matrix $F\rho_{\mathrm{reg}}(g)F^\dagger$ is a block-diagonal matrix, where each block corresponds to $\rho(g)$ for some irreducible representation ρ of G. The Fourier transform is unique, up to a permutation of the blocks and up to a choice of basis for ρ for each irreducible ρ.

Let $\widehat{G}$ denote the set of all inequivalent irreducible representations of G. For a representing ρ let d_ρ denote the dimension of ρ. We define a transform F by

$$F\left|g\right\rangle \;=\; \sum_{\rho\in\widehat{G}}\sum_{1\le i,j\le d_\rho}\sqrt{\frac{d_\rho}{|G|}}\rho_{i,j}(g)\left|\rho,i,j\right\rangle.$$

This transformation is unique up to a choice of a unitary map between $\mathrm{Span}\left\{\left|\rho,i,j\right\rangle : \rho\in\widehat{G},\ 1\le i,j\le d_\rho\right\}$ and $\mathrm{Span}\left\{\left|g\right\rangle : g\in G\right\}$.

The following analysis shows that F is indeed a Fourier transform, in the sense that it block diagonalizes the regular representations (where each $\{\left|\rho,i,j\right\rangle\left\langle\rho,i',j\right| : 1\le i,i'\le d_\rho\}$ corresponds to a block).

$$\begin{aligned}
F\rho_{\mathrm{reg}}(g)F^\dagger &= \sum_{x\in G}\sum_{\rho,\rho'\in\widehat{G}}\sum_{1\le i,j\le d_\rho;\ 1\le i',j'\le d_{\rho'}}\frac{\sqrt{d_\rho d_{\rho'}}}{|G|}\rho_{i,j}(gx)\overline{\rho'_{i',j'}(x)}\left|\rho,i,j\right\rangle\left\langle\rho',i',j'\right| \\
&= \sum_{x\in G}\sum_{\rho,\rho'\in\widehat{G}}\sum_{1\le i,j\le d_\rho;\ 1\le i',j'\le d_{\rho'}}\frac{\sqrt{d_\rho d_{\rho'}}}{|G|}\sum_{1\le k\le d_\rho}\rho_{i,k}(g)\rho_{k,j}(x)\overline{\rho'_{i',j'}(x)}\left|\rho,i,j\right\rangle\left\langle\rho',i',j'\right| \\
&= \sum_{\rho,\rho'\in\widehat{G}}\sum_{1\le i,j\le d_\rho;\ 1\le i',j'\le d_{\rho'}}\sum_{1\le k\le d_\rho}\rho_{i,k}(g)\left(\frac{\sqrt{d_\rho d_{\rho'}}}{|G|}\sum_{x\in G}\rho_{k,j}(x)\overline{\rho'_{i',j'}(x)}\right)\left|\rho,i,j\right\rangle\left\langle\rho',i',j'\right| \\
&= \sum_{\rho,\rho'\in\widehat{G}}\sum_{1\le i,j\le d_\rho;\ 1\le i',j'\le d_{\rho'}}\sum_{1\le k\le d_\rho}\rho_{i,k}(g)\delta_{\rho,\rho'}\delta_{k,i'}\delta_{j,j'}\left|\rho,i,j\right\rangle\left\langle\rho',i',j'\right| \\
&= \sum_{\rho\in\widehat{G}}\sum_{1\le i,i',j\le d_\rho}\rho_{i,i'}(g)\left|\rho,i,j\right\rangle\left\langle\rho,i',j\right|
\end{aligned}$$

In the above analysis we have used the great orthogonality theorem, which states that

$$\frac{\sqrt{d_\rho d_{\rho'}}}{|G|}\sum_{x\in G}\rho_{i,j}(x)\overline{\rho'_{i',j'}(x)} = \delta_{\rho,\rho'}\delta_{i,i'}\delta_{j,j'}.$$

3 Quantum expanders from non-Abelian Cayley graphs

As we said before, our quantum expander takes two steps on a Cayley expander (over the group PGL(2,q)) with a basis change between each of the steps, and the basis change is a carefully chosen transformation.

First, in Subsection 3.1, we define and analyze taking one step on a (Abelian or non-Abelian) Cayley graph. Then, in Subsection 3.2 we analyze the Abelian case. We do not use the results of Subsection 3.2 for analyzing PGL(2,q), but never the less we recommend reading this section because many of its techniques are later on generalized to the non-Abelian case. Then, we study a general template for constructing quantum expanders over non-Abelian groups with a certain property (Subsections 3.3, 3.4). Finally, we show that PGL(2,q) has this required property (Subsection 3.5).

3.1 A single step on a Cayley graph

We now fix an arbitrary (Abelian or non-Abelian) group G of order N, and a subset S of group elements closed under inverse. The *Cayley graph* associated with S, $C(G,S)$, is a graph over $|G|$ elements, with an edge between (g_1,g_2) iff $g_1 = g_2 s$ for some $s\in S$. $C(G,S)$ is a regular directed graph of degree $|S|$. It is undirected because S is closed under inverse. It is connected iff S is a set of generators. Rather then thinking of the Cayley graph as a graph, we prefer to think of it as a linear operator over $\mathbb{C}[G]$. We associate the graph with the operator that is its normalized adjacency matrix M (the normalization is such that the operator norm is 1). This operator is thus $M = \frac{1}{|S|}\sum_{s\in S} |xs\rangle\langle x|$ [1].

Notice that $M = C(G,S)$ is a symmetric operator, and therefore diagonalizes with real eigenvalues. We denote by $\lambda_1 \geq \ldots \geq \lambda_N$ the eigenvalues of M with orthonormal eigenvectors $v_1,\ldots,v_N$ (i.e., $\| v_i \|_2 = 1$). As M is regular, we have $\lambda_1 = 1$ and $\overline{\lambda} = \max_{i>1}|\lambda_i| \leq 1$.

We now define our basic superoperator $T : L(\mathbb{C}[G]) \to L(\mathbb{C}[G])$. The superoperator has a register S of dimension $|S|$ that is initialized at $\left|\overline{0}\right\rangle$. It does the following:

- It first applies Hadamard on register S (getting into the density matrix $\frac{1}{|S|}\rho \otimes \sum_{s,s'} |s\rangle\langle s'|$).
- Then, it applies the unitary transformation $U : |g,s\rangle \to |gs,s\rangle$. This transformation is a permutation over the standard basis, and hence unitary. It is also classically easy to compute in both directions, and therefore has an efficient quantum circuit.
- Finally, it measures register S.

Thus we have: $T(\rho) = \mathrm{Tr}_S[\, U(I\otimes H)(\rho \otimes \left|\overline{0}\right\rangle\left\langle\overline{0}\right|)(I\otimes H)U^\dagger \,]$.

We begin by identifying the eigenvectors and eigenvalues of T. We may think of an eigenvector $v_i \in \mathbb{C}^N$ as an element of $\mathbb{C}[G]$, $|v_i\rangle = \sum_g v_i(g)\,|g\rangle$. We also define the linear transformation $R : \mathbb{C}[G] \to L(\mathbb{C}[G])$ by $R\,|g\rangle = |g\rangle\langle g|$. With this notation we define:

$$\mu_{i,g} \;=\; \rho_{\mathrm{reg}}(g)(R\,|v_i\rangle) \;=\; \sum_{x\in G} v_i(x)\,|gx\rangle\langle x|$$

Lemma 3.1. *The vectors $\{\mu_{i,g} \mid i = 1,\ldots,N, g\in G\}$ form an orthonormal basis of $L(\mathbb{C}[G])$, and $\mu_{i,g}$ is an eigenvector of T with eigenvalue $\lambda_{i,g} = \lambda_i$.*

Proof. We first notice that $T(|g_1\rangle\langle g_2|) = \mathrm{Tr}_S[\frac{1}{|S|}\sum_{s_1,s_2} U\,|g_1,s_1\rangle\langle g_2,s_2|\,U^\dagger] = \frac{1}{|S|}\sum_s |g_1 s\rangle\langle g_2 s|$. [2] Now,

$$\begin{aligned}
T(\mu_{i,g}) &= T(\sum_x v_i(x)\,|gx\rangle\langle x|) \;=\; \sum_x v_i(x) T(|gx\rangle\langle x|) \\
&= \frac{1}{|S|}\sum_{x,s} v_i(x)\,|gxs\rangle\langle xs| \;=\; \frac{1}{|S|}\sum_{x,s} v_i(x)\rho_{\mathrm{reg}}(g)\,|xs\rangle\langle xs| \\
&= \rho_{\mathrm{reg}}(g)\frac{1}{|S|}\sum_{x,s} v_i(x)\,|xs\rangle\langle xs| \;=\; \rho_{\mathrm{reg}}(g)R(\sum_x v_i(x)\frac{1}{|S|}\sum_s |xs\rangle) \\
&= \rho_{\mathrm{reg}}(g)R(\sum_x v_i(x)M\,|x\rangle) \\
&= \rho_{\mathrm{reg}}(g)R(M(\sum_x v_i(x)\,|x\rangle)) \;=\; \rho_{\mathrm{reg}}(g)R(M\,|v_i\rangle) \\
&= \rho_{\mathrm{reg}}(g)\cdot R(\lambda_i\,|v_i\rangle) \;=\; \lambda_i\rho_{\mathrm{reg}}(g)R(|v_i\rangle) \;=\; \lambda_i\mu_{i,g}.
\end{aligned}$$

[1] In our definition the generators act from the right. Sometimes the Cayley graph is defined with left action, i.e., g_1 is connected to g_2 iff $g_1 = sg_2$. However, note that if we define the invertible linear transformation P that maps the basis vector $|g\rangle$ to the basis vector $|g^{-1}\rangle$, then $PMP^{-1} = PMP$ maps x to $\frac{1}{|S|}\sum_s |(x^{-1}s)^{-1}\rangle = \frac{1}{|S|}\sum_s |s^{-1}x\rangle = \frac{1}{|S|}\sum_s |sx\rangle$ and so the right action is M and the left action is PMP^{-1}, and therefore they are similar and in particular have the same spectrum.

[2] We remark that if we think of T as an operator over $\mathbb{C}[G\times G]$ (identifying $|x\rangle\langle y|$ with $|x,y\rangle$) then T itself is a Cayley graph with the set of operators being $\{(s,s) \mid s\in S\}$. Furthermore, if we look at $W = \{(g,g) \mid g\in G\}$ then W is a subgroup of $G\times G$ and W is invariant under T. In general, for every $(g_1,g_2)\in G\times G$, the left coset $(g_1,g_2)W = \{(g_1 g, g_2 g) \mid g\in G\}$ is invariant under T.

To see orthonormality notice that for $g_1 \neq g_2$, $\mathrm{Tr}(\mu_{i,g}\mu^{\dagger}_{i',g'}) = 0$ simply because for all (k,ℓ) for at least one of the matrices the (k,ℓ) entry is zero. If $g_1 = g_2 = g$ then $\mathrm{Tr}(\mu_{i,g}\mu^{\dagger}_{i',g'}) = \langle v_{i'}|v_i\rangle = \delta_{i,i'}$. As the number of vectors $\{\mu_{i,g}\}$ is N^2 they form an orthonormal basis for $L(\mathbb{C}[G])$. ☐

Given $v \in \mathbb{C}[G]$ we can decompose it and express it as $v = v^{||} + v^{\perp}$ where $v^{||} \in \mathrm{Span}\{|v_1\rangle\}$ and $v^{\perp} \in \mathrm{Span}\{|v_2\rangle, \ldots, |v_N\rangle\}$. In analogy, for $A \in L(\mathbb{C}[G])$ we can decompose it to $A = A^{||} + A^{\perp}$ where $A^{||} \in \mu^{||} = \mathrm{Span}\{\mu_{1,g} \mid g \in G\}$ and $A^{\perp} \in \mu^{\perp} = \mathrm{Span}\{\mu_{i,g} \mid i \neq 1, g \in G\}$. Notice that T has eigenvalue λ_i on $\mu_{i,g}$ and so in particular has eigenvalue $1 = \lambda_1$ on $\mu^{||}$. Also, let us denote $\overline{\lambda} = \max_{i\neq 1}|\lambda_i|$. We have:

Claim 3.1. *For any $A \in \mu^{\perp}$, $\| T(A) \|^2 \leq \overline{\lambda}^2 \| A \|^2$.*

Proof. Express $A = \sum_{i\neq 1,g}\beta_{i,g}\mu_{i,g}$. Then $\| A \|^2 = \sum_{i\neq 1,g}|\beta_{i,g}|^2$ and $T(A) = \sum_{i\neq 1,g}\beta_{i,g}\lambda_i\mu_{i,g}$. In particular, $\| T(A) \|^2 = \sum_{i\neq 1,g}|\beta_{i,g}|^2|\lambda_i|^2 \leq \overline{\lambda}^2 \| A \|^2$. ☐

3.2 The Abelian Expander

In this section we describe a quantum expander based on a Cayley graph of an Abelian group, G. When G is Abelian, all the irreducible representations are of dimension 1 and these are the group characters [3]. There are exactly $|G|$ different characters, and we can associate each $g \in G$ with a character χ_g such that $\chi_g(x) = \chi_x(g)$. We associate each character χ with the norm one vector $|\chi_g\rangle = \frac{1}{\sqrt{N}}\sum_x \chi_g(x)|x\rangle$ in $\mathbb{C}[G]$. The eigenvectors of the Cayley graph are exactly the set of characters $|v_g\rangle = |\chi_g\rangle$.

We now describe the quantum expander. We let U be the Fourier transform over G, i.e., the unitary transformation mapping $|g\rangle$ to $|\chi_g\rangle$. Our expander is the superoperator

$$E(\rho) = T(UT(\rho)U^{\dagger}).$$

We claim:

Claim 3.2. $U\mu_{g,i}U^{\dagger} = \chi_i(g^{-1}) \cdot \mu_{i,g^{-1}}$.

Proof.

$$\begin{aligned}
U\mu_{g,i}U^{\dagger} &= U\rho_{\mathrm{reg}}(i)R\,|\chi_g\rangle\,U^{\dagger} \;=\; \frac{1}{\sqrt{N}}\sum_x \chi_g(x)U\,|ix\rangle\langle x|\,U^{\dagger} \\
&= \frac{1}{\sqrt{N}}\sum_x \chi_g(x)\,|\chi_{ix}\rangle\langle\chi_x| \\
&= \frac{1}{N\sqrt{N}}\sum_{x,y,y'} \chi_g(x)\chi_{ix}(y)\overline{\chi_x(y')}\,|y\rangle\langle y'| \\
&= \frac{1}{\sqrt{N}}\sum_{y,y'} \chi_i(y)\;\left[\,\frac{1}{N}\sum_x \chi_x(gyy'^{-1})\,\right]\;|y\rangle\langle y'| \\
&= \frac{1}{\sqrt{N}}\sum_{y'} \chi_i(g^{-1}y')\,|g^{-1}y'\rangle\langle y'| \\
&= \chi_i(g^{-1})\cdot\rho_{\mathrm{reg}}(g^{-1})R\,|\chi_i\rangle \;=\; \chi_i(g^{-1})\cdot\mu_{i,g^{-1}}
\end{aligned}$$

☐

We claim:

Lemma 3.2. *E is a $(|S|^2, \overline{\lambda})$ quantum expander.*

[3] A character is a homomorphism from G to $\mathbb{C}$, .i.e., a function $\chi : G \to \mathbb{C}$ such that $\chi(g_1g_2) = \chi(g_1)\chi(g_2)$.

Proof. It is easy to check that $E(\tilde{I}) = \tilde{I}$. Furthermore, fix any $\rho \in D(\mathbb{C}[G])$ that is perpendicular to $\tilde{I}$. Write $\rho = \rho^{||} + \rho^{\perp}$ where $\rho^{||} \in W = \mathrm{Span}\{\mu_{1,g} \mid 1 \neq g \in G\}$ and $\rho^{\perp} \in \mu^{\perp}$. Given Claim 3.2 one can verify that $E(\rho^{||}) \perp E(\rho^{\perp})$. In particular

$$\begin{aligned} ||E(\rho)||^2 &= ||E(\rho^{||})||^2 + ||E(\rho^{\perp})||^2 \\ &\leq ||T(U\rho^{||}U^{\dagger})||^2 + ||T(\rho^{\perp})||^2 \\ &\leq \overline{\lambda}^2 ||\rho^{||}||^2 + \overline{\lambda}^2 ||\rho^{\perp}||^2 \ = \ \overline{\lambda}^2 ||\rho||^2. \end{aligned}$$

The first inequality is due to the fact that T has eigenvalue 1 on $\rho^{||}$ and both T and U have operator norm at most 1. The second inequality is by Claims 3.2 and 3.1.

The seed bound comes from the fact that the superoperator E traces out exactly $2\log|S|$ registers, and thus can increase its input's entropy by at most $2\log|S|$. □

3.3 Template for a quantum expander over a general group

In this subsection we show how to construct a quantum expander over any group G that possess some general property. We later show that the $\mathrm{PGL}(2, q)$ group possesses this property.

Similar to the Abelian case, the expander will be of the form

$$E(\rho) = T(UT(\rho)U^{\dagger}),$$

where U will be the Fourier transform over G. Unlike the Abelian case, in the non-Abelian case G has many representations of dimension greater than 1. Thus, a significant part of describing U will be to describe the basis for each one of the ρ_{reg}-invariant subspaces. The property that we need from the unitary transformation U is:

Definition 3. *We say U is a* good basis change *if for any $g_1 \neq 1$ it holds that*

$$\mathrm{Tr}(U\rho_{\mathrm{reg}}(g_1)U^{\dagger}\rho_{\mathrm{reg}}(g_2)) \;=\; 0. \tag{1}$$

The intuition behind this choice is as follows. As before, let $W = \mathrm{Span}\{\rho_{\mathrm{reg}}(g) : g \neq 1 \in G\}$ be the set of eigenvectors of T with eigenvalue 1 (besides the identity). Since each of these eigenvectors was not shrunk by T in the first step, it is necessary to move them into a perpendicular subspace, such that the second step will shrink them. If U is a good basis change this indeed happens as captured in:

Claim 3.3. *If $\rho \in W$ and U is a good basis change then $U\rho U^{\dagger} \perp \mu^{||}$*

Proof. $\{\rho_{\mathrm{reg}}(g) : g \in G\}$ is an orthonormal basis for $\mu^{||}$. $\{\rho_{\mathrm{reg}}(g) : g \neq 1 \in G\}$ is an orthonormal basis for W. Therefore, it is enough to verify that $\mathrm{Tr}(U\rho_{\mathrm{reg}}(g_1)U^{\dagger}\rho_{\mathrm{reg}}(g_2)^{\dagger}) = 0$ for any $g_1 \neq 1$ and for any g_2. Since $\rho_{\mathrm{reg}}(g_2)^{\dagger} = \rho_{\mathrm{reg}}(g_2^{-1})$, this follows directly from Property (1). □

We claim:

Lemma 3.3. *If U is a good basis change then E is a $(|S|^2, \overline{\lambda})$ quantum expander.*

Proof. It is easy to check that $E(\tilde{I}) = \tilde{I}$. Furthermore, fix any $\rho \in D(\mathbb{C}[G])$ that is perpendicular to $\tilde{I}$. Write $\rho = \rho^{||} + \rho^{\perp}$ where $\rho^{||} \in W = \mathrm{Span}\{\mu_{1,g} \mid 1 \neq g \in G\}$ and $\rho^{\perp} \in \mu^{\perp}$. Now it is not true any more that $E(\rho^{||}) \perp E(\rho^{\perp})$. However, we know that $T(\rho^{||}) \perp T(\rho^{\perp})$, and therefore so do $\sigma^{||} = UT(\rho^{||})U^{\dagger}$ and $\sigma^{\perp} = UT(\rho^{\perp})U^{\dagger}$, $\sigma^{||} \perp \sigma^{\perp}$. Also, by Claim 3.3 $\sigma^{||} \perp \mu^{||}$. Thus, by Lemma 2.1:

$$
\begin{aligned}
||E(\rho)||^2 &= ||T(\sigma^{||} + \sigma^{\perp})||^2 \\
&\leq \overline{\lambda}^2 ||\sigma^{||}||^2 + ||\sigma^{\perp}||^2 \\
&= \overline{\lambda}^2 ||UT(\rho^{||})U^{\dagger}||^2 + ||UT(\rho^{\perp})U^{\dagger}||^2 \\
&= \overline{\lambda}^2 ||T(\rho^{||})||^2 + ||T(\rho^{\perp})||^2 \\
&\leq \overline{\lambda}^2 ||\rho^{||}||^2 + \overline{\lambda}^2 ||\rho^{\perp}||^2 \; = \; \overline{\lambda}^2 ||\rho||^2 .
\end{aligned}
$$

The seed bound comes from the fact that the superoperator E traces out exactly $2\log|S|$ registers, and thus can increase its input's entropy by at most $2\log|S|$. □

3.4 A combinatorial property that guarantees Property (1)

Let H be a subgroup of G and let T be a right transversal for H. Then any group element $g \in G$ can be expressed uniquely as $g = h \cdot t$ such that $h \in H$ and $t \in T$. We denote the *coset* of g by $\mathrm{coset}(g) = \mathrm{coset}_{H,T}(g) = t$ and the *index* of g in the coset by $\mathrm{index}(g) = \mathrm{index}_{H,T}(g) = h \in H$.

Definition 4. *Let f be a bijection from $\left\{(\rho, i, j) \mid \rho \in \widehat{G}, 1 \leq i, j \leq d_\rho\right\}$ to G. We say that f is* consistent *if there exists a tower of subgroups $G \geq H_1 \geq \ldots \geq H_k$ and a matching set of right transversals $T_1, \ldots, T_k$ such that for any $\rho \in \widehat{G}$ there exists $1 \leq z \leq k$, and the following holds:*

- *(Every copy of ρ is contained in some coset) $\mathrm{coset}_{i,j} = \mathrm{coset}_{H_z,T_z}(f(\rho, i, j))$ is independent of i, and,*
- *(Different copies of ρ are placed in the same indices) $\mathrm{index}_{i,j} = \mathrm{index}_{H_z,T_z}(f(\rho, i, j))$ is independent of j.*

Another, equivalent, formulation of consistency, is that for any $\rho \in \widehat{G}$ there exists $1 \leq z \leq k$ such that

$$
f(\rho, i, j) \quad = \quad h_i t_j \tag{2}
$$

for some $h_i \in H_z$, $t_j \in T_z$, $i, j = 1, \ldots, d_\rho$.

Observe that wether f is consistent or not depends on the subgroup structure of G, as well as the number and dimension of the irreducible representations of G. It does not depend, however, on the *actual* irreducible representations of G. We now give two examples.

Example 3.1. *(Abelian groups). Any bijection is consistent because all irreducible representations are of dimension one.*

Example 3.2. *(The dihedral group) The Dihedral group D_m is the group of rotations and reflections of a regular polygon with m sides. Its generators are r, the rotation element, and s, the reflection element. This group has $2m$ elements and the defining relations are $s^2 = 1$ and $srs = r^{-1}$. We shall argue this group has a consistent mapping for odd m (although it is true for even m as well). The Dihedral group has $\frac{m-1}{2}$ representations ρ_ℓ of dimension two and two representations of dimension one τ_1, τ_2.*

Our consistent mapping $f(\rho, i, j)$ is:

$$
f(\rho, i, j) \quad = \quad \begin{cases} 1 & \text{If } \rho = \tau_1, i = j = 1 \\ s & \text{If } \rho = \tau_2, i = j = 1 \\ r^{2(\ell-1)+i} s^j & \text{If } \rho = \rho_\ell \end{cases}
$$

To see that f is consistent we look at the cyclic group $H = Z_m = \left\{1, r, \ldots, r^{m-1}\right\}$ of D_m and its transversal $T = \{1, s\}$. For the consistency we see that if ρ is one-dimensional there is nothing to prove. If

ρ is two-dimensional, each of the two copies of ρ ($j = 1, 2$) is mapped into a coset, and for every i, the two copies get the same index $r^{2(\ell-1)+i}$ within the coset. Therefore f is consistent. One can also see directly that Equation (2) is satisfied.

We note that we could have chosen another mapping f' that is consistent with respect to the subgroup $\{1, s\}$ and its transversal set $\{1, r, \ldots, r^{m-1}\}$.

Our claim is that any group that has a consistent mapping can be used to construct quantum expanders. The parameters of the expander depend on the parameters of the classical Cayley graph given by the group. Optimally, we will want a group that has:

- A constant degree Cayley expander.
- A consistent mapping.
- An efficient quantum Fourier transform.

Abelian groups have the last two. In the next section we will show that PGL(2,q) has the first two (it is an open problem to find an efficient implementation of the quantum Fourier transform over PGL(2,q)).

Lemma 3.4. *Let G be a group that has a consistent mapping f, and let F be the Fourier transform over G, $F|g\rangle = \sum_{\rho\in\widehat{G}}\sum_{1\le i,j\le d_\rho}\sqrt{\frac{d_\rho}{|G|}}\rho_{i,j}(g)|\rho,i,j\rangle$. Define the unitary mapping*

$$S \quad : \quad |\rho,i,j\rangle \mapsto \omega_{d_\rho}^{ij}|f(\rho,i,j)\rangle$$

where $\omega_{d_\rho} = e^{2\pi i/d_\rho}$, and set U to be the unitary transformation $U = SF$. Then U has property (1) and is a good basis change.

Before we proceed to the formal proof we give an intuitive explanation. We will see that we can focus separately on the contribution of each irreducible representation ρ. Say the d_ρ copies of ρ appear consistently in cosets of H. If $g_2 \notin H$ we immediately get zero contribution, because entry-wise $U\rho_{\mathrm{reg}}(g_1)U^\dagger$ (which is block-diagonal with blocks that are contained in cosets of H) and $\rho_{\mathrm{reg}}(g_2)$ (which

has non-zero elements only outside H blocks) do not have an entry where both are non-zero. Notice that here we used the fact that each copy of ρ is inside a coset of H. If, on the other hand, $g_2 \in H$, we use the second part of consistency, saying that different copies of ρ have the same index within H. Then, we get sums over d_ρ elements, with only changing phases, and the phases were engineered such that they sum up to 0. We now give formal details.

Proof.

$$\begin{aligned}
\mathrm{Tr}\left(U\rho_{\mathrm{reg}}(g_1)U^\dagger\rho_{\mathrm{reg}}(g_2)\right) &= \mathrm{Tr}\left(SF\rho_{\mathrm{reg}}(g_1)F^\dagger S^\dagger\rho_{\mathrm{reg}}(g_2)\right)\\
&= \mathrm{Tr}\left(S\sum_{\rho\in\widehat{G}}\sum_{1\le i,i',j\le d_\rho}\rho_{i,i'}(g_1)|\rho,i,j\rangle\langle\rho,i',j|S^\dagger\sum_x|g_2x\rangle\langle x|\right)\\
&= \sum_{\rho\in\widehat{G}}\sum_{1\le i,i'\le d_\rho}\rho_{i,i'}(g_1)\,\mathrm{Tr}\left(\sum_{j=1}^{d_\rho}S|\rho,i,j\rangle\langle\rho,i',j|S^\dagger\sum_x|g_2x\rangle\langle x|\right).
\end{aligned}$$

Therefore, it suffices to show that for any ρ, i, i' we have $\mathrm{Tr}\left(\sum_{j=1}^{d_\rho}S|\rho,i,j\rangle\langle\rho,i',j|S^\dagger\sum_x|g_2x\rangle\langle x|\right) = 0$. Fix $\rho\in\widehat{G}$ and $i,i'\in\{1,\ldots,d_\rho\}$. Since f is consistent, there exists a subgroup H and its transversal set T such that $f(\rho,i,j) = h_it_j$ with $h_i\in H$ and $t_j\in T$. Therefore, the sum we need to calculate can be written as

$$
\begin{aligned}
\mathrm{Tr}\left(\sum_{j=1}^{d_\rho} S\,|\rho,i,j\rangle\langle\rho,i',j|\,S^\dagger \sum_x |g_2x\rangle\langle x|\right) &= \sum_{j=1}^{d_\rho}\sum_x \omega_{d_\rho}^{ij-i'j}\,\mathrm{Tr}\left(|h_it_j\rangle\,\langle h_{i'}t_j\,|\,g_2x\rangle\,\langle x|\right) \\
&= \sum_{j=1}^{d_\rho}\sum_x \omega_{d_\rho}^{ij-i'j}\,\langle x\,|\,h_it_j\rangle\,\langle h_{i'}t_j\,|\,g_2x\rangle \\
&= \sum_{j=1}^{d_\rho} \omega_{d_\rho}^{(i-i')j}\left\langle g_2\,|\,h_{i'}h_i^{-1}\right\rangle.
\end{aligned}
$$

where the last equality is because we get a non-zero value iff $x = h_it_j$ and $h_{i'}t_j = g_2x$, which happens iff $h_it_j = g_2^{-1}h_{i'}t_j$, i.e., $g_2 = h_{i'}h_i^{-1}$. However, when $g_2 = h_{i'}h_i^{-1}$ we get the sum $\sum_{j=1}^{d_\rho}\omega_{d_\rho}^{(i-i')j}$. This expression itself is zero when $i \neq i'$.

We are therefore left with the case $i = i'$. In this case $g_2 = h_{i'}h_i^{-1} = 1$. But then,

$$
\mathrm{Tr}\left(U\rho_{\mathrm{reg}}(g_1)U^\dagger\rho_{\mathrm{reg}}(g_2)\right) = \mathrm{Tr}\left(U\rho_{\mathrm{reg}}(g_1)U^\dagger\right) = \mathrm{Tr}\left(\rho_{\mathrm{reg}}(g_1)\right) = 0,
$$

where the last equality follows because $g_1 \neq 1$. □

3.5 The construction of the PGL(2,q) quantum expander

We work with the group $G = \mathrm{PGL}(2,q)$ of all 2×2 invertible matrices over $\mathbb{F}_q$ modulo the group center (the set of scalar matrices). This is one of the groups used by [LPS88] to construct Ramanujan expander graphs. We shall use the template from the previous section to construct our expander. Thus, all that is left to show is that G has a consistent mapping.

The irreducible representations of this group are:

- $\frac{q-3}{2}$ representations of dimension $q+1$.
- $\frac{q-1}{2}$ representations of dimension $q-1$.
- 2 representations of dimension q.
- 2 representations of dimension 1.

We denote by ρ_x^d the xth representation of dimension d (these are all non-equivalent irreducible representations).

Among the various subgroups of $\mathrm{PGL}(2,q)$ we are interested in the group H_1 generated by the equivalence classes of $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ and of $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. H_1 is a Dihedral subgroup of G with $2q$ elements. The first matrix is the reflection, denoted by s, and the second is the rotation, denoted by r). This group has a cyclic subgroup $H_2 = Z_q$ (the group generated by r).

Let $\ell = \frac{(q-1)(q+1)}{2}$ and let $T_1 = \{t_1,\ldots,t_\ell\}$ be a transversal for H_1 (its size comes from the fact that $|G| = q(q-1)(q+1) = 2q\ell$). It follows that $T_2 = \{t_1, st_1,\ldots,t_\ell, st_\ell\}$ is a transversal for H_2.

Our consistent mapping f is defined as follows.

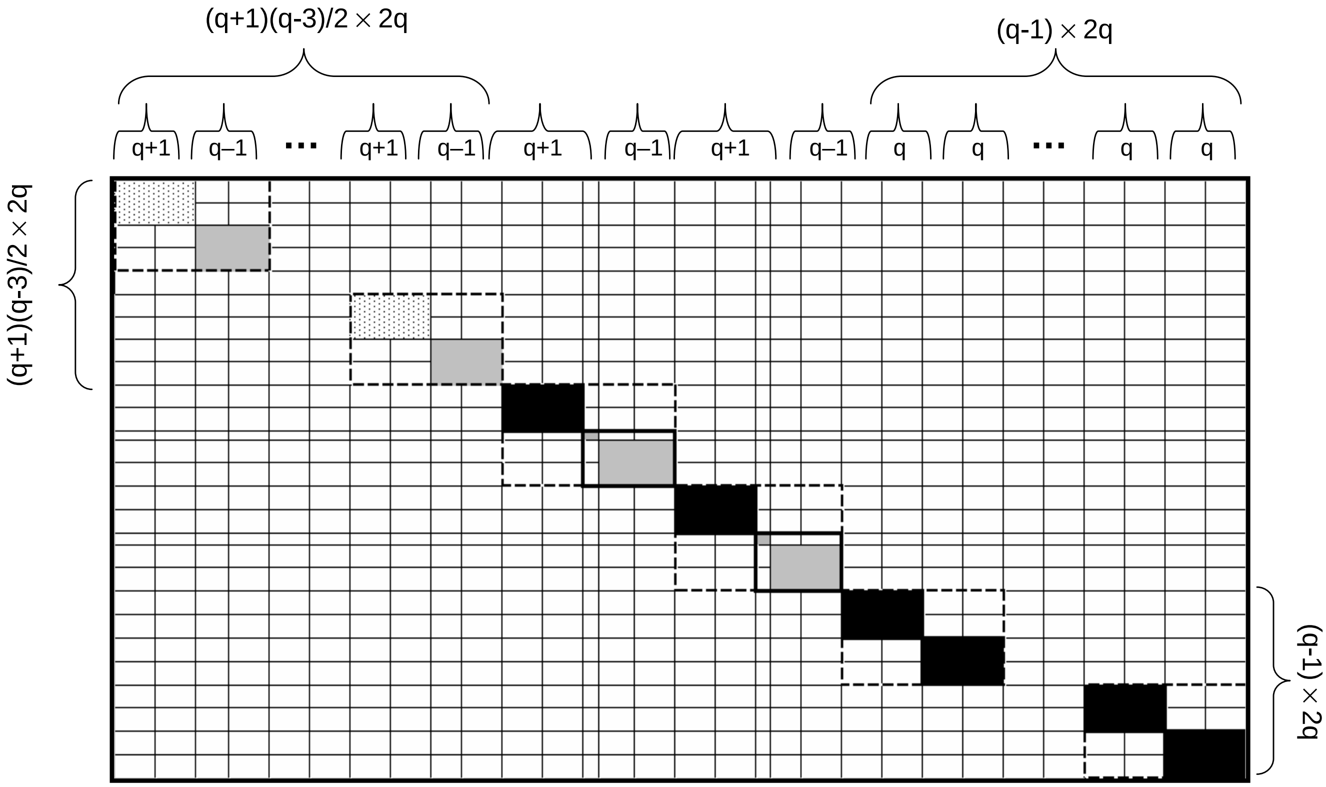

Figure 1: The consistent mapping of PGL(2,q).

$$
\begin{aligned}
f(\rho_x^1, 1, 1) &= st_{x+\frac{(q-3)(q+1)}{2}} \\
f(\rho_x^{q-1}, i, j) &= r^i st_{(x-1)(q-1)+j} \\
f(\rho_x^{q}, i, j) &= \begin{cases} r^{i-1} t_{(x-1)q+j+\frac{(q-3)(q+1)}{2}} & (x-1)q+j \le q+1 \\ r^{i-1} st_{(x-1)q+j-q+1+\frac{(q-3)(q+1)}{2}} & \text{otherwise} \end{cases} \\
f(\rho_x^{q+1}, i, j) &= \begin{cases} r^{i-1} t_{(x-1)(q+1)+j} & i \le q \\ st_{(x-1)(q+1)+j} & i = q+1 \end{cases}
\end{aligned}
$$

In Figure 1 we show this consistent mapping visually. The figure shows the block-diagonal structure of the regular representation (after applying the Fourier transform). Each rectangle is an irreducible representation. Each color represents a different dimension: black rectangles correspond to irreducible representations of dimension q, gray rectangles correspond to irreducible representations of dimension $q-1$ and dotted rectangles correspond to irreducible representations of dimension $q+1$. Notice that all rectangles fit into larger block diagonal rectangles of dimension $2q$, marked with dashed lines. These larger rectangles correspond to cosets of H_1. It is straightforward to verify that for any $q+1$ dimensional representation (dotted rectangles in the figure), the consistency condition is satisfied by H_1 and that for any other representation (black and gray rectangles in the figure), the consistency condition is satisfied by H_2.

We are ready to prove Theorem 1.1:

Proof. (Of Theorem 1.1) By Lemma 3.3, Lemma 3.4 and the description of the consistent mapping above, we know that E is a $(|S|^2, \overline{\lambda})$ quantum expander.

By the [LPS88] construction we know that there exists a Cayley graph for $\mathrm{PGL}(2,q)$ with $\overline{\lambda}^2 \le \frac{4}{|S|}$.

Plugging this Cayley graph gives us a $(\frac{16}{\overline{\lambda}^4}, \overline{\lambda})$ quantum expander. $\square$

4 QED is in QSZK

4.1 Entropy Approximation

In QEA we get one circuit Q and a given threshold t. The yes instances are those with $S(|Q\rangle) \geq t + \frac{1}{2}$ and the no instances are those with $S(|Q\rangle) \leq t - \frac{1}{2}$. The promise problem QEA is a sub problem of QED. Never the less, as in the classical setting, if QEA $\in$ QSZK then so does QED, we give the proof in Section 7. Our proof follows the classical case, and uses the closure under formula which we prove for the quantum case in Section 6. Notice that we do not have a reduction from QED to QEA, but rather the assertion that if QEA is in QSZK then so does QED. We now turn to showing that QEA $\in$ QSZK. It suffices to prove:

4.2 QEA $\leq \overline{\text{QSD}}$

We first give the classical intuition why EA reduces to SD. We are given a circuit C and we want to distinguish between the cases the distribution it defines has substantially more or less than t entropy. First assume that the distribution is flat, i.e., all elements that have a non-zero probability in the distribution, have equal probability. In such a case we can apply an extractor on the n output bits of C, hashing it to about k output bits. If the input distribution has high entropy, it also has high min-entropy (because for flat distributions entropy is the same as min-entropy) and therefore the output of the extractor is close to uniform. If, on the other hand, the circuit entropy is less than $k-d-1$, where d is the extractor seed length, than even after applying the extractor the output distribution has at most $k-1$ entropy, and therefore it must be far away from uniform. We get a reduction to $\overline{\text{SD}}$.

Of course there are a few gaps to complete. First, our source is not necessarily flat. This is solved in the classical case by taking many independent copies of the circuit, which makes the output distribution ”close” to ”nearly-flat” (exact parameters will be given soon). Also, we need to amplify the gap we have between entropy $t+1$ and $t-1$ to a gap larger than d (the seed length). This can also be done by taking many independent copies of C, because $S(C^{\otimes q}) = qS(C)$.

In the quantum case, however, we need to tackle a new problem: we need to find the quantum analogue of a classical extractor. Our Definition 2 is exactly what is needed here, and indeed the problem of showing that QEA $\leq$ $\overline{\text{QSD}}$ lead us to our definition. Also, as we discussed before, we only know how to build *balanced* extractors, and not unbalanced ones (and we even suspect these do not exist). Never the less balanced extractors are sufficient for the proof, which we give below.

We start with flattening the matrix:

Definition 5. *Let ρ be a density matrix, λ an eigenvalue of ρ and Δ a positive number. We say that λ is* Δ-typical *if* $2^{-S(\rho)-\Delta} \leq \lambda \leq 2^{-S(\rho)+\Delta}$.

Definition 6. *A density matrix ρ is* Δ-flat *if for every $t > 0$, a measurement of ρ in its eigenvector basis results an eigenvector with eigenvalue which is $t\Delta$-typical with probability $\geq 1 - 2^{-t^2+1}$.*

Lemma 4.1. *Let ρ be a density matrix and k a positive integer. Suppose that every non-zero eigenvalue of ρ is at least 2^{-m}. Then $\otimes^k \rho$ is Δ-flat for $\Delta = \sqrt{k}m$.*

Proof. Let $\{\lambda_1, \ldots, \lambda_n\}$ denote the set of eigenvalues of ρ. This implies the eigenvalues of $\otimes^k \rho$ are $\{\lambda_{i_1,\ldots,i_k} : \lambda_{i_1,\ldots,i_k} = \lambda_{i_1} \cdot \ldots \cdot \lambda_{i_k}\}$. The entropy of $\otimes^k \rho$ is $S(\otimes^k \rho) = k \cdot S(\rho)$. Let A denote the set of $t\Delta$-typical eigenvalues of $\otimes^k \rho$. Thus $A = \left\{\lambda_{i_1,\ldots,i_k} : |\sum_{j=0}^{k} -\log \lambda_{i_j} - k \cdot S(\rho)| \leq t\Delta\right\}$. Let p denote the probability that a measurement of $\otimes^k \rho$ in its eigenvector basis results an eigenvalue which is not

$t\Delta$-typical. Then by Hoeffding inequality,

$$p \leq \sum_{x \notin A} x \leq 2\exp\left(\frac{-2 \cdot k \cdot (t\Delta/k)^2}{m^2}\right) \leq 2\exp(-2t^2) \leq 2^{-t^2+1}.$$

$\square$

Claim 4.1. *QEA reduces to $\overline{QSD}$.*

Proof. Let (Q, t) be an input to QEA, where Q is a quantum circuit with n input qubits and m output qubits. We first look at the circuit $Q^{\otimes q}$ (for some $q = \text{poly}(n)$ to be specified later). We apply an extractor on the output of $Q^{\otimes q}$. Specifically, let E be a $(qt, q(m-t) + 2\log(\frac{1}{\epsilon}) + \log(qm) + O(1), \epsilon)$ quantum extractor operating on qm qubits, where $\epsilon = 1/\text{poly}(n)$ will be fixed later. Such an extractor exists by Lemma 1.1 and Lemma 1.2. Let $\xi = E(|Q\rangle^{\otimes q})$ and let $\tilde{I} = 2^{-qm} I$. The output of the reduction is $(\xi, \tilde{I})$.

Claim 4.2. *If $(Q, t) \in$ QEA$_Y$ then $\left\| \xi - \tilde{I} \right\|_{\text{tr}} \leq 5\epsilon$.*

Proof. Since Q traces out at most n qubits, the eigenvalues of $|Q\rangle$ are all at least 2^{-n}, we get by Lemma 4.1 that $|Q\rangle^{\otimes q}$ is Δ-flat for $\Delta = \sqrt{q}n$. Thus, with probability at least $1 - 2^{-r^2+1}$, a measurement of $|Q\rangle$ in its eigenvector basis results an eigenvector with eigenvalue which is $r\Delta$-typical. Let Λ denote the set of $r\Delta$-typical eigenvalues of $|Q\rangle$, for $r = \sqrt{\log(\frac{1}{\epsilon})}$. We write $|Q\rangle^{\otimes q}$ in its eigenvector basis $|Q\rangle^{\otimes q} = \sum_i \lambda_i |v_i\rangle\langle v_i|$. Let $\sigma_0 = \sum_{\lambda_i \in \Lambda} \lambda_i |v_i\rangle\langle v_i|$, and let $\sigma_1 = \rho^{\otimes q} - \sigma_0$. Thus, $\text{Tr}(\sigma_0) \geq 1 - 2^{-r^2+1}$. Therefore,

$$\begin{aligned}
\left\| \xi - \tilde{I} \right\|_{\text{tr}} &= \left\| E(\sigma_0) + E(\sigma_1) - \text{Tr}(\sigma_0)\tilde{I} - \text{Tr}(\sigma_1)\tilde{I} \right\|_{\text{tr}} \\
&\leq \left\| E(\sigma_0) - \text{Tr}(\sigma_0)\tilde{I} \right\|_{\text{tr}} + \| E(\sigma_1) \|_{\text{tr}} + \left\| \text{Tr}(\sigma_1)\tilde{I} \right\|_{\text{tr}} \\
&\leq \left\| E(\frac{1}{\text{Tr}(\sigma_0)}\sigma_0) - \tilde{I} \right\|_{\text{tr}} + 2^{-r^2+2}.
\end{aligned}$$

Now we use the fact that $\frac{1}{\text{Tr}(\sigma_0)}\sigma_0$ is a density matrix with all its eigenvalues $\leq 2^{-q \cdot S(\rho) + r\Delta} \cdot \frac{1}{\text{Tr}(\sigma_0)} \leq 2^{-q \cdot S(\rho) + r\Delta + 1}$. Thus, $\frac{1}{\text{Tr}(\sigma_0)}\sigma_0$ has min-entropy at least $q \cdot S(\rho) - r\Delta - 1 \geq q \cdot (t+1) - r\Delta - 1$ since we started with a yes instance for QEA$_Y$. We set the parameters such that $q \geq r\Delta + 1$, and thus our density matrix has min-entropy at least qt and by the guarantee of our quantum extractor we get that $\left\| E(\frac{1}{\text{Tr}(\sigma_0)}\sigma_0) - \tilde{I} \right\|_{\text{tr}} \leq \epsilon$. Therefore, $\left\| \xi - \tilde{I} \right\|_{\text{tr}} \leq \epsilon + 2^{-r^2+2} \leq 5\epsilon$, where the last inequality holds for $r \geq \sqrt{\log(\frac{1}{\epsilon})}$. $\square$

Claim 4.3. *If $(Q, t) \in$ QEA$_N$ then $\left\| \xi - \tilde{I} \right\|_{\text{tr}} \geq \frac{1}{qm} - \frac{1}{2^{qm}}$.*

Proof. Suppose that $(Q, t) \in$ QEA$_N$. By the definition of quantum extractors we get that

$$\begin{aligned}
S(\xi) &\leq S(|Q\rangle^{\otimes q}) + q(m-t) + 2\log(\frac{1}{\epsilon}) + \log(qm) + O(1) \\
&\leq q(t-1) + q(m-t) + 2\log(\frac{1}{\epsilon}) + \log(qm) + O(1) \\
&= qm - q + 2\log(\frac{1}{\epsilon}) + \log(qm) + O(1) \leq qm - 1,
\end{aligned}$$

where the last inequality follows if we choose the parameters such that $q > 2\log(\frac{1}{\epsilon}) + \log(qm) + O(1)$. By Lemma 5.1 we get that $\left\| \xi - \tilde{I} \right\|_{\text{tr}} \geq \frac{1}{qm} - \frac{1}{2^{qm}}$ as required. $\square$

The constraints we have on the parameters are $q \geq \sqrt{\log(\frac{1}{\epsilon})}\sqrt{q}n+1$ and $q > 2\log(\frac{1}{\epsilon})+\log(qm)+O(1)$. To this we add $5\epsilon < \left(\frac{1}{qm} - \frac{1}{2^{qm}}\right)^2$. This ensures a gap which can be amplified by Theorem 2.1 to any desired gap, which completes the proof. These constraints can be easily satisfied by choosing q and ϵ^{-1} to be appropriately large polynomials in n.

□

5 Relating entropy to trace distance from the completely mixed state

Now we relate the distance of a density matrix from uniform to a bound on its entropy. Consider the following classical random variable X over $\{0,1\}^n$: with probability ϵ, X samples the fixed string 0^n and with probability $1-\epsilon$, X is uniformly distributed over $\{0,1\}^n$. This X has distance about ϵ from uniform ($\epsilon + \frac{1-\epsilon}{2^n} - \frac{1}{2^n}$ to be exact) and its entropy is $S(\rho) \leq (1-\epsilon)n + H(1-\epsilon)$. We show that this is essentially the worst possible:

Lemma 5.1. *Let ρ be a density matrix over n qubits and $\epsilon > 0$. If $S(\rho) \leq (1-\epsilon)n$ then $\left\| \rho - \frac{1}{2^n}I \right\|_{\text{tr}} \geq \epsilon - \frac{1}{2^n}$.*

Proof. We prove the counter-positive. Let ρ be a density matrix with $\left\| \rho - \frac{1}{2^n}I \right\|_{\text{tr}} < \epsilon - \frac{1}{2^n}$ and minimal Shannon entropy. Writing ρ in its eigenvector basis we get $\rho = \sum_{i=1}^{2^n} \lambda_i \left|v_i\right\rangle\!\left\langle v_i\right|$. W.l.o.g let us assume λ_1 is the largest eigenvalue of ρ. The trace distance of ρ from $\frac{1}{2^n}I$ is $\frac{1}{2}\sum_i |\lambda_i - \frac{1}{2^n}|$. For any eigenvalue $\lambda_i > \frac{1}{2^n}$, where $i \neq 1$, we can modify the eigenvalues of ρ such that $\lambda_1 \leftarrow \lambda_1 + (\lambda_i - \frac{1}{2^n})$ and $\lambda_i \leftarrow \frac{1}{2^n}$. Since both λ_1 and λ_i are $\geq \frac{1}{2^n}$, this does not affect $\left\| \rho - \frac{1}{2^n}I \right\|_{\text{tr}}$. Moreover, we claim this operation only decreases $S(\rho)$:

Lemma 5.2. *Let $\rho = \sum_{i=1}^{2^n} \lambda_i \left|v_i\right\rangle\!\left\langle v_i\right|$ be a density matrix over n qubits with eigenvalues $(\lambda_1 \geq \ldots \geq \lambda_{2^n})$. Let $\lambda_j > \epsilon > 0$ for some $j > 1$. Let $\delta_1 = \lambda_1 + \epsilon$, $\delta_j = \lambda_j - \epsilon$ and $\delta_i = \lambda_i$ for $i \neq 1, j$ and let $\sigma = \sum_{i=1}^{2^n} \delta_i \left|v_i\right\rangle\!\left\langle v_i\right|$. Then $S(\rho) \geq S(\sigma)$.*

We prove the lemma shortly. Thus, w.l.o.g. we can assume $\lambda_i \leq 2^{-n}$ for all $i > 1$. Having that $\left\| \rho - \tilde{I} \right\|_{\text{tr}} = \sum_{i:\lambda_i > 2^{-n}} \lambda_i - 2^{-n} = \lambda_1 - 2^{-n}$. As $\left\| \rho - \tilde{I} \right\|_{\text{tr}} \leq \epsilon - 2^{-n}$ we conclude that $\lambda_1 \leq \epsilon$. It follows that

$$S(\rho) \geq \sum_{i>1} \lambda_i \log(\lambda_i^{-1}) \geq \sum_{i>1} \lambda_i \cdot n > (1-\epsilon)n.$$

which completes the proof. □

Proof. (Of Lemma 5.2) $f(x) = x\log x^{-1}$ is concave. Therefore, for $\lambda_j = \delta_j + \epsilon = (1 - \frac{\epsilon}{\delta_1 - \delta_j})\delta_j + \frac{\epsilon}{\delta_1 - \delta_j}\delta_1$ we get: $f(\lambda_j) \geq (1 - \frac{\epsilon}{\delta_1 - \delta_j})f(\delta_j) + \frac{\epsilon}{\delta_1 - \delta_j}f(\delta_1)$. Similarly, $f(\lambda_1) \geq \frac{\epsilon}{\delta_1 - \delta_j}f(\delta_j) + (1 - \frac{\epsilon}{\delta_1 - \delta_j})f(\delta_1)$. Together, $f(\lambda_j) + f(\lambda_1) \geq f(\delta_j) + f(\delta_1)$. Therefore,

$$\begin{aligned} S(\rho) - S(\sigma) &= \lambda_1 \log \lambda_1^{-1} + \lambda_j \log \lambda_j^{-1} - \delta_1 \log \delta_1^{-1} - \delta_j \log \delta_j^{-1} \\ &= f(\lambda_1) + f(\lambda_j) - f(\delta_1) - f(\delta_j) \geq 0. \end{aligned}$$

□

6 Closure under boolean formula

In order to prove that QED reduces to QSD we need to generalize another classical result about SZK to QSZK, namely, closure under boolean formula. A special case of this is, e.g., that if $\Pi \in$ QSZK then the promise problem that accepts (x_1, x_2) if $x_1 \in \Pi_{yes}$ or $x_2 \in \Pi_{yes}$ and rejects if both x_i are in Π_{no}, is also in QSZK. Notice that as we deal with promise problems we have yes instances and no instances and also ”undefined” instances, and therefore we need to say how to treat those ”undefined” instances in our formula. We define:

Definition 7. *For a promise problem* Π*, the* characteristic function *of* Π *is the map* $\chi_\Pi : \{0,1\}^* \to \{0,1,\star\}$ *given by*

$$\chi_\Pi(x) = \begin{cases} 1 & \textit{if } x \in \Pi_Y \\ 0 & \textit{if } x \in \Pi_N \\ \star & \textit{otherwise} \end{cases}$$

and,

Definition 8. *A* partial assignment *to variables* $v_1, \ldots, v_k$ *is* k*-tuple* $\overline{a} = (a_1, \ldots, a_k) \in \{0,1,\star\}^k$*. For a propositional formula* ϕ *on variables* $v_1, \ldots, v_k$ *the evaluation* $\phi(\overline{a})$ *is recursively defined as follows:*

$$v_i(\overline{a}) = a_i, \qquad (\phi \wedge \psi)(\overline{a}) = \begin{cases} 1 & \textit{if } \phi(\overline{a}) = 1 \textit{ and } \psi(\overline{a}) = 1 \\ 0 & \textit{if } \phi(\overline{a}) = 0 \textit{ or } \psi(\overline{a}) = 0 \\ \star & \textit{otherwise} \end{cases}$$

$$(\neg\phi)(\overline{a}) = \begin{cases} 1 & \textit{if } \phi(\overline{a}) = 0 \\ 0 & \textit{if } \phi(\overline{a}) = 1 \\ \star & \textit{otherwise} \end{cases} \qquad (\phi \vee \psi)(\overline{a}) = \begin{cases} 1 & \textit{if } \phi(\overline{a}) = 1 \textit{ or } \psi(\overline{a}) = 1 \\ 0 & \textit{if } \phi(\overline{a}) = 0 \textit{ and } \psi(\overline{a}) = 0 \\ \star & \textit{otherwise} \end{cases}$$

Notice that, e.g., $0 \wedge \star = 0$ even though one of the inputs is ”undefined” in Π.

With that we define:

Definition 9. *For any promise problem* Π*, we define a new promise problem* $\Phi(\Pi)$ *as follows:*

$$\begin{aligned} \Phi(\Pi)_Y &= \{(\phi, x_1, \ldots, x_m) : \phi(\chi_\Pi(x_1), \ldots, \chi_\Pi(x_m)) = 1\} \\ \Phi(\Pi)_N &= \{(\phi, x_1, \ldots, x_m) : \phi(\chi_\Pi(x_1), \ldots, \chi_\Pi(x_m)) = 0\} \end{aligned}$$

The following is an adaptation of the classical proof of [SV98] to the quantum setting:

Theorem 6.1. *For any promise problem* $\Pi \in$ *QSZK,* $\Phi(\Pi) \in$ *QSZK.*

Proof. Let Π be any promise problem in QSZK. Since QSD is QSZK-complete, Π reduces to QSD. This induces a reduction from $\Phi(\Pi)$ to $\Phi(\text{QSD})$. Thus, it suffice to show that $\Phi(\text{QSD})$ reduces to QSD.

Claim 6.1. $\Phi($*QSD*$)$ *reduces to QSD.*

Proof. Let $w = (\phi, (X_0^1, X_1^1), \ldots, (X_0^m, X_1^m))$ be an instance of $\Phi(\text{QSD})$. By applying De Morgan’s Laws, we may assume that the only negations in ϕ are applied directly to the variables. (Note that De Morgan’s Laws still hold in our extended boolean algebra.) By the polarization lemma (Theorem 2.1) and by the closure of QSZK under complement (as was shown by [Wat02]), we can construct in polynomial time pairs of circuits $(Y_0^1, Y_1^1), \ldots, (Y_0^m, Y_1^m)$ and $(Z_0^1, Z_1^1), \ldots, (Z_0^m, Z_1^m)$ such that:

$$\begin{aligned} (X_0^i, X_1^i) \in \text{QSD}_Y &\Rightarrow \left\| \left|Y_0^i\right\rangle - \left|Y_1^i\right\rangle \right\|_{\text{tr}} \geq 1 - \frac{1}{3|\phi|} \text{ and } \left\| \left|Z_0^i\right\rangle - \left|Z_1^i\right\rangle \right\|_{\text{tr}} \leq \frac{1}{3|\phi|} \\ (X_0^i, X_1^i) \in \text{QSD}_N &\Rightarrow \left\| \left|Y_0^i\right\rangle - \left|Y_1^i\right\rangle \right\|_{\text{tr}} \leq \frac{1}{3|\phi|} \text{ and } \left\| \left|Z_0^i\right\rangle - \left|Z_1^i\right\rangle \right\|_{\text{tr}} \geq 1 - \frac{1}{3|\phi|} \end{aligned}$$

The reduction outputs the pair of circuits $(\text{BuildCircuit}(\phi, 0), \text{BuildCircuit}(\phi, 1))$, where BuildCircuit is the following recursive procedure:

BuildCircuit(ψ, b)

1. If $\psi = v_i$, output Y_b^i.
2. if $\psi = \neg v_i$, output Z_b^i.
3. If $\psi = \tau \vee \mu$, output BuildCircuit$(\tau, b) \otimes$ BuildCircuit(μ, b).
4. If $\psi = \tau \wedge \mu$, output $\frac{1}{2}$(BuildCircuit$(\tau, 0) \otimes$ BuildCircuit$(\mu, b)) + \frac{1}{2}$(BuildCircuit$(\tau, 1) \otimes$ BuildCircuit$(\mu, 1-b))$.

Notice that the number of recursive calls equals the number of sub-formula of ϕ, and therefore the procedure runs in time polynomial in $|\psi|$ and $|X_i^j|$, i.e., polynomial in its input length.

We now turn to proving correctness by induction. For a sub-formula τ of ϕ, let

$$\Delta(\tau) \quad = \quad \| \left(\text{BuildCircuit}(\tau, 0) - \text{BuildCircuit}(\tau, 1)\right) |0\rangle \, \|_{\text{tr}}$$

We claim:

Claim 6.2. *Let* $\overline{a} = (\chi_{QSD}(X_0^1, X_1^1), \ldots, \chi_{QSD}(X_0^m, X_1^m))$. [4] *For every sub-formula* ψ *of* ϕ*, we have:*

$$\begin{aligned} \psi(\overline{a}) = 1 \quad &\Rightarrow \quad \Delta(\psi) \geq 1 - \frac{|\psi|}{3|\phi|} \\ \psi(\overline{a}) = 0 \quad &\Rightarrow \quad \Delta(\psi) \leq \frac{|\psi|}{3|\phi|} \end{aligned}$$

Proof. By induction on the sub-formula of ϕ. It holds for atomic sub-formula by the properties of the Y's and Z's.

- The case $\psi = \tau \vee \mu$.

  If $\psi(\overline{a}) = 1$ then either $\tau(\overline{a}) = 1$ or $\mu(\overline{a}) = 1$. W.l.o.g., say $\tau(\overline{a}) = 1$. In this case we have for any $i \in \{0, 1\}$ that BuildCircuit$(\tau, i) = \mathcal{E}$ (BuildCircuit(ψ, i)), where $\mathcal{E}$ is the quantum operation tracing out the registers associated with the μ sub-formula. Thus, by Fact 2.5 and by induction,

  $$\Delta(\psi) \geq \Delta(\tau) \geq 1 - \frac{|\tau|}{3|\phi|} \geq 1 - \frac{|\psi|}{3|\phi|}.$$

  If $\psi(\overline{a}) = 0$, then both $\tau(\overline{a}) = \mu(\overline{a}) = 0$.

  Using

  $$\begin{aligned} \| \rho_0 \otimes \rho_1 - \sigma_0 \otimes \sigma_1 \|_{\text{tr}} \quad &\leq \quad \| \rho_0 \otimes \rho_1 - \sigma_0 \otimes \rho_1 \|_{\text{tr}} + \| \sigma_0 \otimes \rho_1 - \sigma_0 \otimes \sigma_1 \|_{\text{tr}} \\ &= \quad \| \rho_0 - \sigma_0 \|_{\text{tr}} + \| \rho_1 - \sigma_1 \|_{\text{tr}} \,. \end{aligned}$$

  we get

  $$\Delta(\psi) \leq \Delta(\tau) + \Delta(\mu) \leq \frac{|\tau|}{3|\phi|} + \frac{|\mu|}{3|\phi|} \leq \frac{|\psi|}{3|\phi|}.$$

[4] we remind the reader that $\chi_{\text{QSD}}(C_1, C_2)$ was defined in Definition 7.

- The case $\psi = \tau \wedge \mu$.

  Using

$$\begin{aligned} & \left\| \frac{1}{2}[\rho_0 \otimes \sigma_0 + \rho_1 \otimes \sigma_1] - \frac{1}{2}[\rho_0 \otimes \sigma_1 + \rho_1 \otimes \sigma_0] \right\|_{\mathrm{tr}} \\ = \ & \frac{1}{2} \| (\rho_0 - \rho_1) \otimes (\sigma_0 - \sigma_1) \|_{\mathrm{tr}} \ = \ \| \rho_0 - \rho_1 \|_{\mathrm{tr}} \| \sigma_0 - \sigma_1 \|_{\mathrm{tr}} \end{aligned}$$

  where the equalities above follow because $2 \| X \otimes Y \|_{\mathrm{tr}} \ = \ 2 \| X \|_{\mathrm{tr}} 2 \| Y \|_{\mathrm{tr}}$. We get $\Delta(\psi) = \Delta(\tau) \cdot \Delta(\mu)$.

  If $\psi(\overline{a}) = 1$, then, by induction,

$$\Delta(\psi) \geq \left(1 - \frac{|\tau|}{3|\phi|}\right) \left(1 - \frac{|\mu|}{3|\phi|}\right) > 1 - \frac{|\tau| + |\mu|}{3|\phi|} \geq 1 - \frac{|\psi|}{3|\phi|}.$$

  If $\psi(\overline{a}) = 0$, then, w.l.o.g., say $\tau(\overline{a}) = 0$. By induction

$$\Delta(\psi) = \Delta(\tau) \cdot \Delta(\mu) \leq \Delta(\tau) \leq \frac{|\tau|}{3|\phi|} \leq \frac{|\psi|}{3|\phi|}.$$

□

Let $A_b = \text{BuildCircuit}(\phi, b)$. By the above claim if $w \in \Phi(\text{QSD})_Y$ then $\| (A - B) |0\rangle \|_{\mathrm{tr}} \geq 2/3$ and if $w \in \Phi(\text{QSD})_N$ then $\| (A - B) |0\rangle \|_{\mathrm{tr}} \leq 1/3$. Thus the claim follows.

□

□

7 If QEA $\in$ QSZK Then QED $\in$ QSZK.

Proof. By Theorem 6.1, if QEA $\in$ QSZK then $\Phi(\text{QEA}) \in$ QSZK for any formula Φ. Therefore it suffices to show that QED reduces to $\Phi(\text{QEA})$, for some Φ. This is essentially the same reduction which is used by [GSV99] for the classical case.

Claim 7.1. *QED reduces to $\Phi(QEA)$, for some formula Φ.*

Proof. Let (Q_0, Q_1) be an instance of QED. Let $\xi_i = \otimes^6 |Q_i\rangle$. The output of the reduction is

$$\bigvee_{t=1}^{6n} \left[((\xi_0, t) \in \text{QEA}_Y) \wedge ((\xi_1, t) \in \text{QEA}_N) \right].$$

If $(Q_0, Q_1) \in \text{QED}_Y$ then $S(\xi_0) \geq S(\xi_1) + 3$. Thus, there exists an integer t such that $(\xi_0, t) \in \text{QEA}_Y$ and $(\xi_1, t) \in \text{QEA}_N$. On the other hand, if $(Q_0, Q_1) \in \text{QED}_N$ then $S(\xi_1) \geq S(\xi_0) + 3$. Thus, every integer t is either greater than $S(\xi_0) + 1$ or smaller then $S(\xi_1) - 1$. That is, for every t, $(\xi_0, t) \in \text{QEA}_N$ or $(\xi_1, t) \in \text{QEA}_Y$. □

□

8 QSD $\leq$ QED

Theorem 8.1. *For any $0 \leq \alpha < \beta^2 \leq 1$, $QSD_{\alpha,\beta} \leq QED$.*

Proof. Given circuits Q_0, Q_1, We first apply the polarization lemma (Theorem 2.1) with $n = m_0$ and obtain circuits R_0, R_1. We then construct two circuits Z_0 and Z_1 as follows. Z_1 is implemented by a circuit which first applies a Hadamard gate on a single qubit b, measures b and then conditioned on the result it applies either R_0 or R_1. The output of Z_1 is $\frac{1}{2}|0\rangle\langle 0| \otimes |R_0\rangle + \frac{1}{2}|1\rangle\langle 1| \otimes |R_1\rangle$. Z_0 is the same as Z_1 except that b is traced out. The output of Z_0 is $\frac{1}{2}|R_0\rangle + \frac{1}{2}|R_1\rangle$. The output of C is simply a qubit in the completely mixed state.

The reduction outputs the following pair of circuits: $(Z_0 \otimes Z_0 \otimes C, Z_1 \otimes Z_1)$.

The intuition behind the reduction is as follows. First consider the case when $|R_0\rangle$ and $|R_1\rangle$ are very close to each other. the matrix $\frac{1}{2}|R_0\rangle + \frac{1}{2}|R_1\rangle$ is very close both to $|R_0\rangle$ and to $|R_0\rangle$, thus we "lose" the bit of information telling us which circuit was activated. However, the matrix $\frac{1}{2}|0\rangle\langle 0| \otimes |R_0\rangle + \frac{1}{2}|1\rangle\langle 1| \otimes |R_1\rangle$ does contain this bit of information, i.e. has increased entropy. On the other hand, whenever $|R_0\rangle$ and $|R_1\rangle$ are very far, the matrix $\frac{1}{2}|R_0\rangle + \frac{1}{2}|R_1\rangle$ does contain almost the same amount of information as $\frac{1}{2}|0\rangle\langle 0| \otimes |R_0\rangle + \frac{1}{2}|1\rangle\langle 1| \otimes |R_1\rangle$.

Claim 8.1. *If $(Q_0, Q_1) \in (QSD_{\alpha,\beta})_{NO}$ then $(Z_0 \otimes Z_0 \otimes C, Z_1 \otimes Z_1) \in QED_{NO}$*

Proof. We know that $\| |Q_0\rangle - |Q_1\rangle \|_{\mathrm{tr}} \leq \alpha$. By the Polarization lemma (Theorem 2.1) we get $\| |R_0\rangle - |R_1\rangle \|_{\mathrm{tr}} \leq 2^{-m_0}$. By Fact 2.2,

$$S(|Z_1\rangle) = \frac{1}{2}(S(|R_0\rangle) + S(|R_1\rangle)) \ + \ 1.$$

On the other hand, $|Z_0\rangle$ is very close both to $|R_0\rangle$ and to $|R_1\rangle$. Specifically, $\| |Z_0\rangle - |R_1\rangle \|_{\mathrm{tr}} = \| \frac{1}{2}|R_0\rangle - \frac{1}{2}|R_1\rangle \|_{\mathrm{tr}} \leq 2^{-m_0}$. Therefore, by Fannes' inequality (Fact 2.3) $|S(|Z_0\rangle) - S(|R_1\rangle)| \leq 2^{-m_0} \cdot \mathrm{poly}(m_0) \leq 0.1$, for large enough m_0. Similarly, $|S(|Z_0\rangle) - S(|R_0\rangle)| \leq 0.1$. It follows that

$$|S(|Z_0\rangle) - \frac{1}{2}(S(|R_0\rangle) + S(|R_1\rangle))| \leq 0.1.$$

Combining the two equations we get $S(|Z_1\rangle) - S(|Z_0\rangle) \geq 0.9$. Thus, $S(|Z_1 \otimes Z_1\rangle) - S(|Z_0 \otimes Z_0 \otimes C\rangle) \geq 2 * 0.9 - 1 = 0.8$. Therefore, $(Z_0 \otimes Z_0 \otimes C, Z_1 \otimes Z_1) \in \mathrm{QED}_{NO}$ □

Claim 8.2. *If $(Q_0, Q_1) \in (QSD_{\alpha,\beta})_{YES}$ then $(Z_0 \otimes Z_0 \otimes C, Z_1 \otimes Z_1) \in QED_{YES}$*

Proof. By the Polarization lemma (Theorem 2.1) $\| \rho_0 - \rho_1 \|_{\mathrm{tr}} \geq 1 - 2^{-m_0}$. Using the Holevo bound (Lemma 2.3) we get that $S(|Z_0\rangle) \geq \frac{1}{2}[S(\rho_0) + S(\rho_1)] + 1 - H(\frac{1}{2} + \frac{\| \rho_0 - \rho_1 \|_{\mathrm{tr}}}{2}) \geq \frac{1}{2}[S(\rho_0) + S(\rho_1)] + 1 - H(2^{-m_0})$. By Fact 2.2 we know that $S(|Z_1\rangle = \frac{1}{2}(S(\rho_0) + S(\rho_1)) + 1$. Therefore, $S(|Z_1\rangle) - S(|Z_0\rangle) = H(2^{-m_0}) < 0.1$ for sufficiently large m_0.

In particular, $S(|Z_1 \otimes Z_1\rangle) - S(|Z_0 \otimes Z_0 \otimes C\rangle) \leq 2 * 0.1 - 1 = -0.8$ and $(Z_0 \otimes Z_0 \otimes C, Z_1 \otimes Z_1) \in \mathrm{QED}_{YES}$

□

□

9 Open problems and discussion

Several intriguing open problems are raised by our definition of quantum extractors. Our definition applies only to *balanced* extractors (functions from $L(V)$ to $L(V)$). One can easily extend the definition to unbalanced domains. However, it is not clear whether quantum extractors can hash a large domain to a much smaller domain without violating the second condition of Definition 2. It would also be interesting to determine whether quantum extractors (or extensions of them) are applicable for solving the privacy amplification problem [KMR05, Ren05], or not. In addition, it would also be nice to find more applications of quantum extractors.

Our construction of constant seed length extractor also raises many questions. First, the construction is not efficient because we have not shown how to implement the Fourier transform U over PGL(2,q). Second, our construction uses a general property that the underlying group has, which we call a consistent mapping. This property requires a tight connection between the subgroups of the group and its irreducible representations, which we believe is interesting in its own right. Finally, there are other constructions of constant-degree expanders from non-Abelian Cayley graphs (e.g., the recent construction of [Kas05] based on $\mathcal{S}_n$ and $\mathcal{A}_n$) and it is natural to whether these groups have this property. This would be especially useful if the underlying group will have an efficient quantum Fourier transform implementation (such as $\mathcal{S}_n$).

The entropy-loss of a quantum extractor is the difference $k + d - \log(N)$, using the parameters of Definition 2. The construction of [AS04] has $\log n + 2\log(\frac{1}{\epsilon}) + O(1)$ entropy-loss. [AS04] also have a second construction with entropy-loss $2\log(\frac{1}{\epsilon})+O(1)$ but a very large seed d. Our construction has entropy-loss $2(t + \log(\frac{1}{\epsilon}))$. It seems we can gain back most of this entropy-loss using the techniques of [CRVW02]. In fact, one may also view our construction as first doing a small step over a low degree expander, then a permutation (changing the basis) and then a small step over the same low degree expander again, and this approach resembles the zig-zag construction [RVW00]. In fact, even the analysis follows the same line, decomposing to parallel and perpendicular components, where for each one of the components one of the two steps does the job while the other is wasted.

Acknowledgements

We thank Oded Regev for pointing out [AS04] to us and for referring us to Lemma 2.2 that simplified the proof of the reduction from QSD to QED. We also thank Ashwin Nayak, Oded Regev, Adam Smith and Umesh Vazirani for helpful discussions about the paper.

References

[ANTSV02] A. Ambainis, A. Nayak, A. Ta-Shma, and U. V. Vazirani. Quantum dense coding and quantum finite automata. *Journal of the ACM*, 49:496–511, 2002. Earlier version in 31st ACM STOC, 1999, pp. 376-383.

[AS04] A. Ambainis and A. Smith. Small pseudo-random families of matrices: Derandomizing approximate quantum encryption. In *RANDOM*, pages 249–260, 2004.

[CRVW02] M. Capalbo, O. Reingold, S. Vadhan, and A. Wigderson. Randomness conductors and constant-degree expansion beyond the degree/2 barrier. In *Proceedings of the 34th Annual ACM Symposium on Theory of Computing*, pages 659–668, 2002.

[GSV99] O. Goldreich, A. Sahai, and S. P. Vadhan. Can statistical zero knowledge be made non-interactive? or on the relationship of SZK and NISZK. In *CRYPTO*, pages 467–484, 1999.

[GW97] O. Goldreich and A. Wigderson. Tiny families of functions with random properties: A quality-size trade-off for hashing. *Random Structures and Algorithms*, 11(4):315–343, 1997.

[HF91] J. Harris and W. Fulton. *Representation Theory*. Springer, 1991.

[HRTS00] S. Hallgren, A. Russell, and A. Ta-Shma. Normal subgroup reconstruction and quantum computation using group representations. In *STOC*, pages 627–635, 2000.

[Kas05] Martin Kassabov. Symmetric groups and expander graphs, May 28 2005. Comment: 30 pages.

[KMR05] R. Koenig, U. Maurer, and R. Renner. On the power of quantum memory. *IEEE Transaction on Information Theory*, 51(7):2391–2401, 2005.

[LPS88] A. Lubotzky, R. Philips, and P. Sarnak. Ramanujan graphs. *Combinatorica*, 8:261–277, 1988.

[NC00] M. Nielsen and I. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[Ren05] R. Renner. *Security of Quantum Key Distribution*. PhD thesis, Swiss Federal Institute of Technology (ETH) Zurich, 2005.

[RVW00] O. Reingold, S. Vadhan, and A. Wigderson. Entropy waves, the zig-zag product, and new constant-degree expanders and extractors. In *Proceedings of the 41st Annual IEEE Symposium on Foundations of Computer Science*, pages 3–13, 2000.

[Ser77] J. P. Serre. *Linear representations of finite groups*, volume 42 of *Graduate texts in Mathematics*. Springer, 1977.

[SV97] A. Sahai and S. Vadhan. A complete promise problem for statistical zero-knowledge. In *FOCS*, pages 448–457, 1997.

[SV98] A. Sahai and S. Vadhan. Manipulating statistical difference, 1998.

[Wat02] J. Watrous. Limits on the power of quantum statistical zero-knowledge. In *FOCS*, pages 459–470, 2002.

[Wat06] J. Watrous. Zero-knowledge against quantum attacks. In *STOC*, pages 296–305, 2006.